**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**(Attorney Docket No. 15225US01)**

In the Application of:

Sherman (Xuemin) Chen

Serial No. 10/713,415

Filed: November 14, 2003

For: METHOD AND SYSTEM FOR
SECURE KEY GENERATION

Examiner: Longbit Chai

Group Art Unit: 2131

Confirmation No. 2739

Electronic Filing Date:

September 22, 2008

## RESPONSE UNDER 37 C.F.R. § 1.133

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This paper is a written statement of the substance of the telephone interview of September 3, 2008 with the Examiner, in accordance with 37 C.F.R. §1.133 and MPEP §713. The Applicant respectfully requests entry of the following statement, and consideration of the following remarks.

## SUBSTANCE OF INTERVIEW

A telephone interview took place on September 3, 2008. The Applicant had filed an Amendment and a Pre-appeal brief on July 22, 2008, in response to the Final Office Action of April 22, 2008, and the Advisory Action of July 2, 2008. In addition, a telephone interview had been conducted on August 18, 2008, leading to no agreement (see corresponding Substance of Interview Summary). However, an agreement was reached on September 3, 2008.

In the telephone interview, the Examiner suggested several amendments to independent claims 1, 11, 21 and 35, the most important of which was to incorporate an amended form of claim 3 into the independent claims 1 (and similarly for independent claim 11, 21, and 35), which would make the claims allowable. The Examiner also stated that no change to independent claims 31, and 45 would be required to make them allowable.

An oral agreement was reached, and the Applicant provided the below list of agreed-upon changes, which was confirmed by the Examiner via email on September 5, to make all claims allowable.

## AMENDMENT TO THE CLAIMS

Claims 1, 2, 4, 5, 11, 12, 14, 15, 21, 22, 24, 25, 35, 36, 38, and 39 have been amended. Claims 3, 13, 23, and 37 have been cancelled.

**Listing of claims:**

1. (Currently amended) A method for producing a secure key, the method comprising:

receiving a plurality of input keys comprising ~~at least~~ a first input key, a second input key and a third input key; ~~and~~

generating a first output key based on said plurality of input keys comprising ~~at least~~ said first input key, said second input key and said third input key, wherein said first output key is unique and differs from at least one of said plurality of ~~at least said first~~ input ~~key~~keys, and said ~~third input key~~ one of said plurality of input keys is a key variation comprising a device identity; and

continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys.

2. (Currently amended) The method according to claim 1, wherein said first input key is a customer key, and/or ~~said second input key is~~ a customer key selection.

3. (Cancelled)

4. (Currently amended) The method according to claim ~~3~~1, comprising determining whether said ~~second~~ first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

5. (Currently amended) The method according to claim 4, wherein said first output key ~~and said second output key are~~ is not a weak or semi-weak ~~keys~~key.

6. (Previously presented) The method according to claim 1, comprising mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

7. (Previously presented) The method according to claim 6, comprising generating an intermediate key based on said first input key.

8. (Previously presented) The method according to claim 7, comprising scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

9. (Previously presented) The method according to claim 8, comprising:

masking at least a portion of said generated mapped output key data; and

exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

10. (Previously presented) The method according to claim 1, comprising transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

11. (Currently amended) A machine-readable storage having stored thereon, a computer program having at least one code section for producing a secure key, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving a plurality of input keys comprising ~~at least~~ a first input key, a second input key and a third input key; ~~and~~

generating a first output key based on said plurality of input keys comprising ~~at least~~ said first input key, said second input key and said third input key, wherein said first output key is unique and differs from at least one of said plurality of ~~at least said first~~ input ~~key~~keys, and said ~~third input key~~ one of said plurality of input keys is a key variation comprising a device identity; and

continuing said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys.

12. (Currently amended) The machine-readable storage according to claim 11, wherein said first input key is a customer key, and/or ~~said second input key is~~ a customer key selection.

13. (Cancelled)

14. (Currently amended) The machine-readable storage according to claim ~~13~~11, wherein said at least one code section comprises code for determining whether said ~~second~~first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

15. (Currently amended) The machine-readable storage according to claim 14, wherein said first output key ~~and said second output key are~~ is not a weak or semi-weak ~~keys~~key.

16. (Previously presented) The machine-readable storage according to claim 11, wherein said at least one code section comprises code for mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

17. (Previously presented) The machine-readable storage according to claim 16, wherein said at least one code section comprises code for generating an intermediate key based on said first input key.

18. (Previously presented) The machine-readable storage according to claim 17, wherein said at least one code section comprises code for scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

19. (Previously presented) The machine-readable storage according to claim 18, wherein said at least one code section comprises:

code for masking at least a portion of said generated mapped output key data; and

code for exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

20. (Previously presented) The machine-readable storage according to claim 11, wherein said at least one code section comprises code for transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

21. (Currently amended) A system for producing a secure key, the system comprising:

a secure key generator that receives a plurality of input keys comprising ~~at least~~ a first input key, a second input key and a third input key; ~~and~~

said secure key generator generates a first output key based on said plurality of input keys comprising ~~at least~~ said first input key, said second input key and said third input key, wherein said first output key is unique and differs from at least one of said plurality of input keys~~at least said first input key~~, and said ~~third input key~~ one of said plurality of input keys is a key variation comprising a device identity; and

said secure key generator continues said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys.

22. (Currently amended) The system according to claim 21, wherein said first input key is a customer key, and/or ~~said second input key is~~ a customer key selection.

23. (Cancelled)

24. (Currently amended) The system according to claim ~~23~~21, wherein said secure key generator determines whether said ~~second~~first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

25. (Currently amended) The system according to claim 24, wherein said first output key ~~and said second output key are~~ is not a weak or semi-weak ~~keys~~key.

26. (Previously presented) The system according to claim 21, comprising a mapper that maps said at least said first input key, said second input key and said third input key to generate mapped output key data.

27. (Previously presented) The system according to claim 26, comprising a key generator that generates an intermediate key based on said first input key.

28. (Previously presented) The system according to claim 27, comprising a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

29. (Previously presented) The system according to claim 28, comprising:

a masker that masks at least a portion of said generated mapped output key data; and

an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

30. (Original) The system according to claim 21, wherein said secure key generator transfers said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

31. (Original) A system for producing a secure key, the system comprising:

a mapper;

a scrambler coupled to said mapper;

a masker coupled to said mapper;

a key generator coupled to said scrambler; and

an XOR operator coupled to said masker and said scrambler.

32. (Previously presented) The system according to claim 31, comprising at least one processor coupled to an output of said XOR operator.

33. (Previously presented) The system according to claim 32, comprising an encryption engine that is coupled to an output of said XOR operator.

34. (Previously presented) The system according to claim 33, comprising a memory coupled to at least one of said encryption engine and said at least one processor.

35. (Currently amended) A system for producing a secure key, the system comprising:

one or more circuits enabled to:

receive a plurality of input keys comprising ~~at least~~ a first input key, a second input key and a third input key at a secure key generator; ~~and~~

generate at said secure key generator a first output key based on said plurality of input keys comprising ~~at least~~ said first input key, said second input key and said third input key, wherein said first output key is unique and differs from at least one of said plurality of input keys ~~at least said first input key~~, and wherein said one of said plurality of input keys~~third input key~~ is a key variation comprising a device identity; and continue said generating of said first output key via a modified at least one of said plurality of input keys, until said first output key differs from at least one of said plurality of input keys.

36. (Currently amended) The system according to claim 35, wherein said first input key is a customer key, and/or ~~said second input key is~~ a customer key.

37. (Cancelled) The system according to claim 35, wherein said one or more circuits:

determine whether said first output key is at least one of a unique key and differs from said at least said first input key; and

generate a second output key based on a modified one of at least one of said first input key, said second input key and said third input key, if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key.

38. (Currently amended) The system according to claim ~~37~~35, wherein said one or more circuits determine whether said ~~second~~ first output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

39. (Currently amended) The system according to claim 38, wherein said first output key ~~and said second output key are~~ is not a weak or semi-weak ~~keys~~key.

40. (Previously presented) The system according to claim 35, wherein said one or more circuits comprise a mapper that maps said at least said first input key, said second input key and said third input key to generate mapped output key data.

41. (Previously presented) The system according to claim 40, wherein said one or more circuits comprise a key generator that generates an intermediate key based on said first input key.

42. (Previously presented) The system according to claim 41, wherein said one or more circuits comprise a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

43. (Previously presented) The system according to claim 42, wherein said one or more circuits comprise:

a masker that masks at least a portion of said generated mapped output key data; and

an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

44. (Previously presented) The system according to claim 35, wherein said one or more circuits transfer said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

45. (Previously presented) A system for producing a secure key, the system comprising one or more circuits, said one or more circuits enabled to operate as:

a mapper;

a scrambler coupled to said mapper;

a masker coupled to said mapper;

a key generator coupled to said scrambler; and

an XOR operator coupled to said masker and said scrambler.

46. (Previously presented) The system according to claim 45, wherein said one or more circuits comprise at least one processor coupled to an output of said XOR operator.

47. (Previously presented) The system according to claim 46, wherein said one or more circuits comprise an encryption engine that is coupled to an output of said XOR operator.

48. (Previously presented) The system according to claim 47, wherein said one or more circuits comprise a memory coupled to at least one of said encryption engine and said at least one processor.

## CONCLUSION

Based on at least the foregoing, the Applicant believes that all claims 1-48 are in condition for allowance. The Applicant respectfully reserves the right to argue additional reasons to those presented above to support the allowability of claims 1-48.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: September 22, 2008

/Ognyan I. Beremski/

Ognyan I. Beremski, Esq.
Registration No. 51,458
Attorney for Applicant

McANDREWS, HELD & MALLOY, LTD.
500 WEST MADISON STREET, 34TH FLOOR
CHICAGO, ILLINOIS 60661
(312) 775-8000

/ CZF